Advanced Metering Implementation

Addressing Security Risks in DoD Applications

Mr. Peter Virag, Weston Solutions
Mr. Matt Franz, SAIC

WESTON SOLUTIONS®
The Trusted Integrator for Sustainable Solutions

SAIC®
From Science to Solutions

Background

- Weston Solutions awarded design/build task orders for advanced metering for Navy District Washington and Quantico MCB
  - Approximately 1,200 electric meters, 300 mechanical, and 270 data recorders
  - Wired and Wireless network
  - Data Acquisition System
  - *System must meet all DoD Information Assurance Requirements*
- Team
  - SAIC
  - Trimark Associates
  - Energy ICT
  - Electrical Testing Specialists

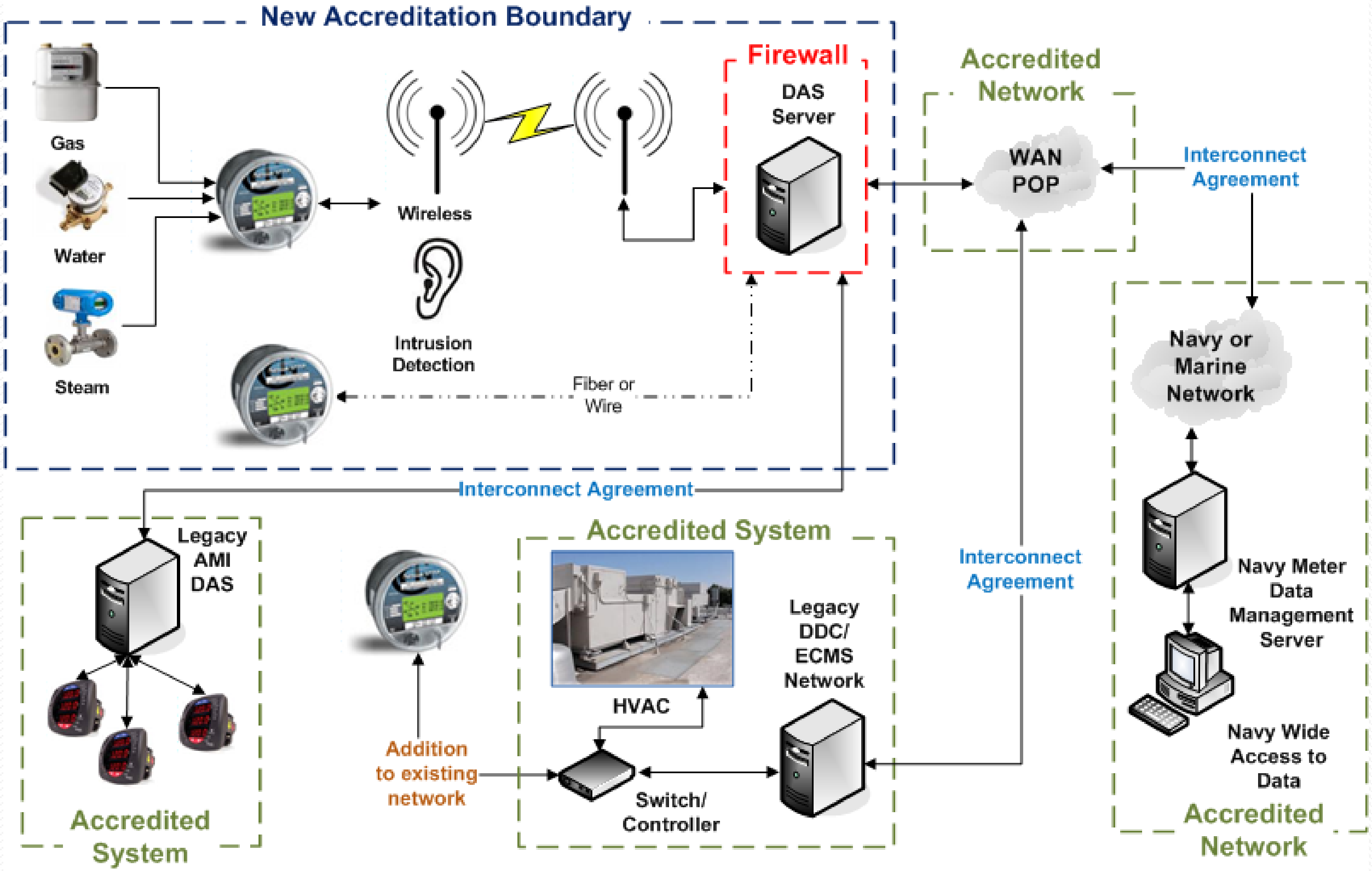
AMI/Smart Grid Security Risks

- Well known application, operating system, and network security vulnerabilities apply to AMI
- Concerns with integrating/sharing AMI network with existing networks
- Sensitivity to disclosure of energy related data, especially for research and operational activities
- Physical security of meters and communications equipment
- Need to balance availability, function, access controls, cost, and usability!
- Partnership approach essential to understand security concerns of client - each case will likely be different

AMI Process: 4 Main Efforts

- Survey and design of physical solution
  - Meter locations
  - Communications Solution
    - Wireless and Wire Network Survey and Design
    - Use of Available Wired and Wireless Network
    - Network addressing and segmentation
    - Physical Limitations
- Customization and Hardening of DAS Solution
  - Customize to meet client data needs
  - Harden to meet Information Assurance requirement
- Security Architecture & System Accreditation
  - Integrated throughout process
  - Involves all hardware/software components and communication flows
  - Required involvement
- Installation and Commissioning

Solution


New Accreditation Boundary
Gas
Water
Steam
Wireless
Intrusion Detection
Fiber or Wire
Firewall
DAS Server
Accredited Network
WAN POP
Interconnect Agreement
Navy or Marine Network
Navy Meter Data Management Server
Navy Wide Access to Data
Accredited Network
Interconnect Agreement
Interconnect Agreement
Legacy AMI DAS
Accredited System
Addition to existing network
Accredited System
HVAC
Legacy DDC/ ECMS Network
Switch/ Controller

Information Assurance: Security & Compliance

- Compliance: DoD Information Assurance Certification and Accreditation Process (DIACAP) Platform Information Technology (PIT)
  - Specific administrative processes and timelines
    - Interim Authority to Test (IATT), Interim Authority to Operate (IATO), Authority to Operate (ATO), etc.
  - Focus on identification and validation of security controls
  - Well defined deliverables that must be created
- Security
  - “Common sense” approach based on a deep understanding of hardware, software, and being deployed
  - “Bottom up” view of realistic assessment of threats, vulnerabilities, controls
  - Interpretation, adaptation, and refinement of processes and documents to Energy Management Systems

Information Assurance: Lessons Learned

- Engineering best practices provide a strong foundation for Information Assurance—*knowing your system is half the battle*
- Teamwork is critical with the solutions and customer teams:
  - Documentation and testing requirements must be identified as early as possible in the process
  - “Full stack” awareness from physical to application layer is critical for secure design, operation, and deployment
- IA can be the “glue” helping to build a functional system vs. the “roadblock” preventing deployment
  - IA personnel must understand Smart Grid/Control Systems Security in addition to “IT” Security
- Existing DoD (DIACAP) and Federal Information Security (FISMA) can (and are!) being applied to Energy Management Systems—comparable to NERC CIP

Thank you!

Questions?

WESTON SOLUTIONS®

The Trusted Integrator for Sustainable Solutions

SAIC®

From Science to Solutions